Mega Financial Holding Co., Ltd. Personal Data File Security Maintenance Guidelines

Amended in the 22nd meeting of the 5th Board of Directors on February 25, 2014
Amended in the 4th meeting of the 6th Board of Directors on September 22, 2015
Amended in the 18th meeting of the 6th Board of Directors on August 23, 2016
The Board of Directors authorized the renaming of the unit on October 27, 2020; the amendments took effect on January 1, 2021
Amended in the 12th meeting of the 8th Board of Directors on May 24, 2022

Chapter 1 General Principles

Article 1 (Purpose and Basis)

The Guidelines are established in accordance with the "Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission" to enhance the Company's personal data file management and ensure personal data security.

Article 1-1 (Responsible Unit)

The Compliance Department is the responsible unit of the Guidelines.

Chapter 2 Planning for Personal Data Protection

Article 2 (Assign Suitable Manpower)

The Compliance Department shall assign suitable management personnel and resources based on the scale and characteristics of the Company's business operations. They shall be responsible for the establishment of the Guidelines and supervision of the units' compliance with the Guidelines and related personal data management mechanisms, procedures, and measures.

The President is authorized to approve the personal data management mechanisms, procedures, and measures in the preceding paragraph.

Article 3 (Periodic Inspections)

All units of the Company must follow the relevant laws and regulations relating to personal data protection. They shall verify and confirm the current status of its retention of personal data and define the scope of security maintenance management established in the Guidelines.

Article 4 (Risk Assessment)

The units of the Company shall assess potential risks to personal data arising from the scope of personal data defined in the foregoing Article and from the

processes of collecting, processing, and using of personal data in the course of the Company's businesses.
Based on the results of such risk assessment, the Compliance Department shall establish an appropriate management mechanism.

Article 5　(Personal Data Incident Response Mechanisms)

To respond to security incidents involving theft, tampering, damage, loss, or leak of personal data (hereafter referred to as "incidents"), the Company shall establish the following mechanisms concerning the responses to, and the reporting and prevention of, incidents:

I. Measures to be adopted in the aftermath of an incident, including:
(I) Ways to mitigate the party's damages.
(II) Appropriate methods to notify the party after investigation of the Incident has been completed.
(III) Inform the party of the facts of the incident, response measures taken, and the hotline for inquiry services.
II. After the occurrence of the incident, the persons to be notified and the methods of notification.
III. After the occurrence of the incident, a discussion mechanism for exploring corrective and preventive measures.

In the event of a major personal data incident, the unit receiving the report shall report the leak of personal data to the Financial Supervisory Commission within 72 hours (holidays are included in the calculation of the duration) in accordance with the format in the attachment for Article 6 of the "Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission". However, if other requirements are specified in other laws and regulations, such requirements shall apply. Any corrective or preventive measures developed by the Company in accordance with Subparagraph 3 of the preceding paragraph shall be analyzed in their entirety and reviewed by experts who are impartial and independent and whose qualifications have been publicly certified.

The term "major personal data incident" mentioned above shall refer to any theft, tampering, damage, loss, or leak of personal data that jeopardizes the Company's normal operations or the rights of a large number of parties.

Article 6　(Training)

The Company shall regularly promote employee awareness of personal data protection and educate and train such employees so that they understand the relevant legal requirements, the scope of their responsibilities, and the various mechanisms, procedures, and measures concerning the protection of personal data related to these Guidelines.

Chapter 3　Personal Data Management Procedures and Measures

Article 7　(Management Procedures)

The Company shall establish personal data management procedures with respect to the following matters:

I. When collecting, processing, or using personal data that contain special personal data as specified in Article 6 of the Personal Data Protection Act, the Company must examine the specified purpose thereof and whether relevant laws and regulations have been complied with; where written consent has been obtained from the party, the Company shall ensure compliance with Article 7, Paragraphs 1, 2, and 4 of the Personal Data Protection Act which apply mutatis mutandis to Article 6, Paragraph 2 of the Act.

II. The Company shall examine whether the collection and processing of personal data is exempt from the requirement of notifying the party, and whether the content and method of notification are lawful and appropriate.

III. The Company shall examine whether the collection and processing of personal data comply with Article 19 of the Personal Data Protection Act, which requires a specified purpose and the satisfaction of one of the statutory circumstances set forth therein; where the party grants approval, it must also ensure compliance with the requirements of Article 7 of the Personal Data Protection Act.

IV. The Company shall examine whether personal data are used within the necessary scope of the specified purpose for collection under Article 20 of the Personal Data Protection Act; if data are used for a purpose other than the specified purpose, the Company shall examine whether such use falls within one of the statutory circumstances; where consent has been obtained from the party, the Company shall ensure compliance with the requirements of Article 7 of the Personal Data Protection Act.

V. When the Company outsources the collection, processing, or use of

personal data to a third party, whether in whole or in part, the Company shall exercise proper supervision over the outsourcing vendor in accordance with Article 8 of the Enforcement Rules of the Personal Data Protection Act, and the contents of such supervision shall be clearly set forth in the outsourcing contract or in relevant documents.

VI. Before transmitting personal data internationally, the Company shall examine whether there are applicable restrictions imposed by the Financial Supervisory Commission, and shall comply accordingly.

VII. Related issues concerning a party's exercise of rights under Article 3 of the Personal Data Protection Act:

(I) Confirmation of the party's identity.

(II) Providing the party with methods through which the party may exercise his/her rights, and informing the party of the charges to be paid and of other matters requiring explanation.

(III) Methods for reviewing the party's requests, and compliance with the processing time limits set forth in the Personal Data Protection Act.

(IV) Where there is a reason as provided under the Personal Data Protection Act to refuse the party's exercise of rights, the recording of such reason and the method of notifying the party.

VIII. The Company shall examine whether the process of collecting, processing, or using personal data is correct; where there are errors or disputes concerning correctness, the matter shall be resolved in accordance with Article 11, Paragraphs 1, 2, and 5 of the Personal Data Protection Act.

IX. The Company shall examine whether the specified purpose with regard to the personal data has become non-existent, or if its time limit has expired; if the specified purpose no longer exists or if the time limit has expired, the Company shall delete, and cease the processing and use of, such information, in accordance with Article 11, Paragraph 3 of the Personal Data Protection Act.

Article 8　(Data Security Management Measures)

The Company shall adopt the following data security management measures to protect the personal data in its possession:

I. Establish rules concerning the use of various types of equipment and storage media, as well as appropriate measures to be adopted to prevent the leak of data when such equipment or media are written off or used for other purposes.

II. With respect to the contents of retained personal data, if encryption is

required, the appropriate encryption measures shall be adopted in the collection, processing or use of such data.

III. Apply proper protection to backup data if there is a procedural need to backup personal data.

Article 9 (Equipment Security Management Measures)

The Company shall adopt the following equipment security management measures for personal data held by the Company and stored on paper, disk, tape, optical disc, microfilm, integrated circuit, computer, automated machinery, or other media:

I. Implement proper access control.

II. Establish appropriate methods for safekeeping media.

III. Install proper protection equipment or technology depending on the specific characteristics and operating environment of the medium.

Article 10 (Personnel management measures)

The Company shall adopt the following personnel management measures to protect the personal data in its possession:

I. All units shall review and confirm the dedicated personnel for all business procedures involving the collection, processing, or use of personal data.

II. All units shall set limits on relevant employees' access to personal data and to control and manage such employees' access.

III. The Company shall enter into an agreement with such employees that establishes an obligation of confidentiality.

Chapter 4 Security Auditing, Record Retention, and Continuous Improvement Mechanisms for Personal Data

Article 11 (Auditing Mechanisms)

To ensure the implementation of the Guidelines and personal data management mechanisms, procedures, and measures, the Auditing Office shall establish an appropriate mechanism for conducting audits on the security of personal data based on the scale and characteristics of the Company's business operations. It shall also incorporate related mechanisms into the internal control and audit items.

Article 12 (Record Retention)

With respect to the personal data protection mechanisms, procedures, and measures established by the Company's units in carrying out the security maintenance of personal data files, the Company must record the uses of the personal data and maintain records or relevant evidence thereof.

After the Company's units delete or cease to process or use personal data held by the Company's pursuant to Article 11, Paragraph 3 of the Personal Data Protection Act, the Company shall retain the following records:

I. The method and timing of the deletion of, or of ceasing to process or use, personal data.
II. When the personal data being deleted, or ceasing to be processed or used, is transferred to another person, the reason, transferee, method, and timing of the transfer, as well as the legal basis for the transferee's collection, processing or use thereof.

Tracking records, relevant evidence, and records mentioned in the preceding two paragraphs shall be retained for at least five years. The foregoing shall not apply where the law or the contract stipulates otherwise.

Article 13 (Self-Evaluation Report)

To continue to maintain personal data security protection, the units of the Company that hold personal data must file a self-evaluation report at least once every year and implement the following matters:

I. Review and amend the Guidelines and related personal data protection matters.
II. Plan and execute improvement and prevention measures if the evaluation report shows any potential violation of laws or regulations.

The self-evaluation report in the preceding paragraph shall be compiled by the Compliance Department and reported to the President for approval.

Chapter 5 Supplementary Provisions

Article 14 (Other Matters)

Matters not specified in the Guidelines shall be governed by applicable laws and regulations and the Company's regulations.

Article 15 (Level of Approval Authority)

These Guidelines shall take effect after being approved by the Board of Directors. The same applies when these Guidelines are revised or revoked.

Format in the attachment for Article 6 of the "Regulations Governing Security and Maintenance of Personal Data Files of Non-government Agency Designated by the Financial Supervisory Commission"

<table>
<tr><td colspan="3">Personal Data Infringement Incident Report and Record Table</td></tr>
<tr><td>Name of the non-government agency:

Reporting agency/unit: _____</td><td colspan="2">Report time: (year) (month) (date) (hour) (minute)
Reported by: Signature (seal)
Title:
Tel:
Email：
Address:</td></tr>
<tr><td>Incident occurrence time</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Incident type</td><td rowspan="2">□Theft
□Leak
□Tampering
□Damage
□Loss
□Other infringements</td><td>Total number of personal data infringements (approximate)</td></tr>
<tr><td>□General personal data: ___ entries
□Special personal data: ___ entries</td></tr>
<tr><td>Reason for the occurrence of the incident and summary</td><td colspan="2"></td></tr>
<tr><td>Status of damage</td><td colspan="2"></td></tr>
<tr><td>Possible outcomes due to leak of personal data</td><td colspan="2"></td></tr>
<tr><td>Proposed response measures</td><td colspan="2"></td></tr>
<tr><td>Proposed time and method for notifying</td><td colspan="2"></td></tr>
</table>

Whether the leak of personal data is reported to the Financial Supervisory Commission within 72 hours after discovery	□ Yes □ No. Reason:

Note 1: If information for a field is not yet known, it may be specified as "unknown" and the information shall be reported and updated when it is known.

Note 2: Holidays are included in the calculation of the duration for the aforementioned reports to the Financial Supervisory Commission within 72 hours.